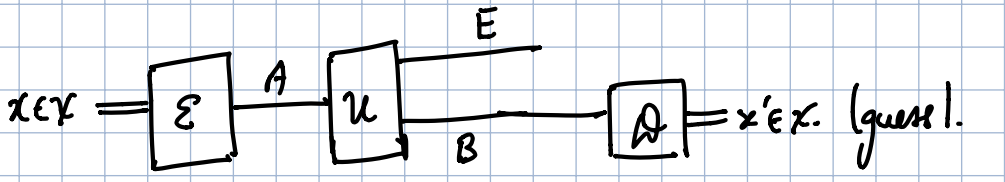
Private classical communication

Goal: Send classical inf. from Alice to Bob while keeping inf. private from an eavesdropper.

Given:

- Quantum channel $\mathcal{N}_{A\to B}$.
- Message set: $\mathcal{X}$, size $|\mathcal{X}|$.
- Local encoding and decoding.
- No ent. assistance



Recall: $\mathcal{N}(\rho) = \mathrm{Tr}_E[U(\rho \otimes |0\rangle\langle 0|)U^\dagger]$. (Alice to Bob)

$\Rightarrow \mathcal{N}^c(\rho) = \mathrm{Tr}_B[U(\rho \otimes |0\rangle\langle 0|)U^\dagger]$ (Alice to eavesdropper).

↑ "complementary" channel.

$$\rho_{X_A X_A'} = \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} |x\rangle\langle x|_{X_A} \otimes |x\rangle\langle x|_{X_A'} \longrightarrow \rho_{X_A A} = \mathcal{E}_{X_A' \to A}(\rho_{X_A X_A'}) = \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} |x\rangle\langle x|_{X_A} \otimes \rho_A^x$$

$$\to \rho_{X_A B E} = \mathcal{U}_{A\to BE}(\rho_{X_A A}) = \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} |x\rangle\langle x|_{X_A} \otimes \tau_{BE}^x$$

$$\to \boxed{\omega_{X_A X_B E} = \mathcal{U}_{B\to X_B}(\omega_{X_A BE}) = \frac{1}{|\mathcal{X}|}\sum_{x,x'\in\mathcal{X}} \mathrm{Tr}_B\left[(M_B^{x'} \otimes \mathbb{1}_E)\tau_{BE}^x\right] |x\rangle\langle x|_{X_A} \otimes |x'\rangle\langle x'|_{X_B}}$$

(final state of the protocol)

Figure of merit: Bob's guess should be close to Alice's sent message: $X_A = X_B$.

$$\boxed{\varepsilon_I} = 1 - \mathrm{Tr}[\Pi_{X_A X_B}\, \omega_{X_A X_B}], \quad \Pi_{X_A X_B} = \sum_{x\in\mathcal{X}} |x\rangle\langle x|_{X_A} \otimes |x\rangle\langle x|_{X_B} \quad (\text{"reliability"})$$

Also, for **privacy**: $\exists\ \sigma_E$ such that $\frac{1}{2}\|\tau_E^x - \sigma_E\|_1 = \boxed{\varepsilon_{II}}\ \forall x\in\mathcal{X}$.

This happens for an ideal $\mathcal{E}$ channel!

(*) Can achieve private communication using <u>secret key + one-time pad</u>

Secret key is a string of iid bits satisfying $p(a,b) = \frac{1}{4}\delta_{a,b}$ $\forall$ bits a,b

So uniformly distributed equal-valued bit strings shared by Alice and Bob that is uncorrelated from any eavesdropper:

$$p(a,b,e) = p(a,b)\,p(e) = \tfrac{1}{2}\delta_{a,b}\,p(e). \longleftrightarrow \underline{\text{secret bit}}$$

<u>One-time pad</u>: $M \oplus K = C \longrightarrow C \oplus K = M$

(M: message, K: key, C: cipher; send C to Bob (copy could go to eavesdropper))

$M_1 \oplus K = C_1$ $C_1 \oplus C_2 = M_1 \oplus K \oplus M_2 \oplus K = M_1 \oplus M_2$ $\Rightarrow$ can only use key once!

- <u>Private comm.</u>: secret key + one-time pad
- <u>Quantum Comm.</u>: entanglement + teleportation

} So secret key is like the classical analogue of entanglement!

↳ <u>Note</u>: Quantum comm. $\Rightarrow$ private comm.

$Q(\mathcal{N}) \leq P(\mathcal{N})$.

Specifically, from max. ent state $(\mathbb{E}^+)_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$, by measuring in $\{|0\rangle,|1\rangle\}$ basis we get the secret-key dist. $p(a,b)$ above.

Also, b/c $|\mathbb{E}^+\rangle$ is pure, any eavesdropper has to be in a <u>product state</u>

$\mathbb{E}^+_{AB} \otimes \sigma_E \Rightarrow p(a,b,e) = p(a,b)\,p(e)$ for any σ_E

So entanglement gives a g. strategy for creating secret key.

(*) Another g strategy for creating secret key: <u>QKD</u> (g. key distribution!)
(specifically prepare-and-measure QKD, which <u>does not require entanglement</u>).

BB84 QKD Protocol

- ✱ Does not use entanglement, but uses concepts of no-cloning and Heisenberg uncertainty relation (measurement of complementary observables).
- ✱ Requires a public authenticated classical channel (eavesdropper can listen to the classical comm., but cannot modify the messages).

- $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

  $|0\rangle \leftrightarrow 0$, $|1\rangle \leftrightarrow 1$: Z-basis (eigenbasis of σ_z)

  $|+\rangle \leftrightarrow 0$, $|-\rangle \leftrightarrow 1$: X-basis (eigenbasis of σ_x)

  ✱ X and Z bases are mutually unbiased: given a state in one basis, measuring in the other basis always gives a uniformly random outcome.

✱ Can think of $|0\rangle, |1\rangle$ as $|H\rangle, |V\rangle$ single photon states and $|\pm\rangle$ as $|\pm 45°\rangle$ single photon states.

- Ideal protocol: Alice and Bob connected by noiseless q. channel (so no eavesdropper).

Alice ——————— Bob

Step 1: Alice picks a basis at random (prob. $\frac{1}{2}$), and sends randomly-chosen state from that basis (prob. $\frac{1}{2}$) to Bob. $\left((b_A, k_A),\ b_A \in \{X, Z\},\ k_A \in \{0, 1\}\right)$

Step 2: Bob picks a basis at random, and measures in that basis $\left((b_B, k_B),\ b_B \in \{X, Z\},\ k_B \in \{0, 1\}\right)$

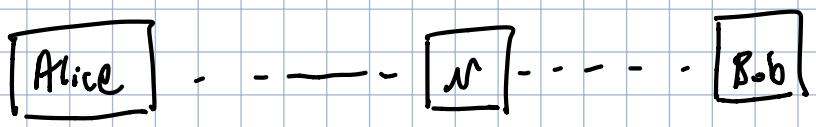
Step 3: Repeat Step 1 + Step 2 many times.

Step 4: Alice and Bob publicly announce their basis choices. $(b_A \stackrel{?}{=} b_B)$.

They discard the data for which $b_A \neq b_B$ do not agree.

For the remaining data, Alice and Bob share a (perfect) secret key in the value of k_A or k_B (i.e., $k_A = k_B$)

- **Protocol over a Noisy Channel**: Eavesdropper given by complementary channel.



✱ Alice and Bob do not necessarily know the q. channel.

Step 1: Alice picks a basis at random (prob. $\frac{1}{2}$), and sends randomly-chosen state from that basis (prob. $\frac{1}{2}$) to Bob. $\left((b_A, k_A),\ b_A \in \{X, Z\},\ k_A \in \{0,1\}\right)$

Step 2: Bob picks a basis at random, and measures in that basis

$$\left((b_B, k_B),\ b_B \in \{X, Z\},\ k_B \in \{0,1\}\right)$$

Step 3: Repeat Step 1 + Step 2 many times.

Step 4: Alice and Bob publicly announce their basis choices. $(b_A \stackrel{?}{=} b_B)$.

They discard the data for which $b_A \neq b_B$ do not agree.

✱ Now, for the remaining data, there might be errors b/c of the q. channel / eavesdropper.

Step 5: Alice and Bob estimate the errors in their remaining data by sacrificing some of their data

✱ Under certain assumptions, it suffices to estimate one value:

Q: the "quantum bit error rate" → average fraction of bits that disagree.

$(0 \leq Q \leq 1)$.

Step 6: Error-correction and privacy amplification — these are key-distillation steps.

- Error-correction → Correct data via public comm.
- Privacy amplification → Shrink key to account for public comm. in EC step.

Main Result: key rate of $\boxed{1-2h_2(Q)}$ is achievable in the asymptotic limit.

key rate = # of secret bits per channel use

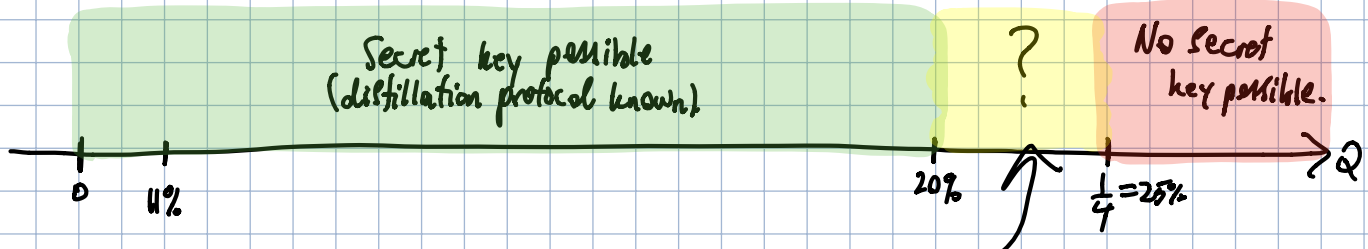
→ This is **not** optimal! This goes to zero at ≃11%, but can tolerate more noise!

How much noise can we in principle tolerate? Find the error in the worst case: Channel is a **replacement channel** (as in classical comm.) This channel is useless for QKD! The replacement channel corresponds to an **intercept-resend attack**: eavesdropper measures the signal being sent and based on the outcome transmits some other state to Bob.

With prob. $\frac{1}{2}$ eavesdropper picks the **wrong** basis, and thus with prob. $\frac{1}{2}$ Bob gets the wrong result (even though both basis choices were same!)

$\Rightarrow \boxed{Q = \frac{1}{4}}$

With prob. $\frac{1}{2}$ eavesdropper picks the **right** basis, does not disturb the state, and Bob picks the right basis, so the data is not discarded



Can secret key be created here? Open problem!